Need to print

US-PAT-NO: 5892899

DOCUMENT-IDENTIFIER: US 5892899 A

TITLE: Tamper resistant methods and apparatus

---------- KWIC ---------

Detailed Description Text - DETX (17):
FIG. 5 illustrates one embodiment of subprogram 204. In accordance with the present invention, for the illustrated embodiment, in addition to original subprogram 102, obfuscated subprogram 204 is provided with mutation partner identification function 206, mutation function 207, partner key 208 and jump block 209. Original subprogram 102 performs a portion of the functions performed by program 100. Original subprogram 102 may be an entry/basis/prologue subprogram 106/108/109 in accordance with the first aspect of the present invention. Mutation partner identification function 206 is used to identify the partner memory cell 202 for all memory cells 202 at each mutation round. In one embodiment, the partner identification function 206 is the function: Partner Cell ID=Cell ID XOR Pseudo-Random Key. For a pseudo-random key, mutation partner identification function 206 will identify a memory cell 202 in the second memory segment 201b as the partner memory cell for of a memory cell 202 in the first memory segment 201a, and vice versa. Only ordered sets of pseudo-random keys that will provide the required periods for the program and its loops will be employed. The length of a period is a function of the pseudo-random keys' set size (also referred to as key length).

Mutation function 207 is used to mutate the content of the various memory cells 202. In one embodiment, mutation function 207 XORs the content of each memory cell 202 in first memory segment 201a into the partner memory cell 202 in second memory segment 201b in an odd mutation round, and XORS the content of each memory cell 202 in second memory segment 201b into the partner memory cell 202 in first memory segment 201a in an even mutation round. Partner key 208 is the pseudo-random key to be used by mutation partner identification function 206 to identify mutation partners of the various memory cells 202 for a mutation round. Jump block 209 transfers execution control to the next obfuscated subprogram 204, which at the time of transfer, has been recovered into plaintext through the pseudo-random pattern of mutations.

Detailed Description Text - DETX (33):

Once mutated, obfuscation processor 214 determines if there are more subprograms 204 to process, step 245. If there are more subprograms 204 to process, obfuscation processor 214 returns to step 234 and proceeds as described earlier. Otherwise, obfuscation processor 214 inserts the mutation partner identification function 206, the partner key to be used to identify mutation partner memory cells, the mutation function, the jump block, and the address of the next subprogram 204 into each of the obfuscated subprograms 204, step 246. Finally, obfuscation processor 214 computes the initial values of the various obfuscated subprograms 204, and outputs them, steps 247-248.